424 Rec'd PCT/PTO 26 MAY 2000

FORM PTO-1390 U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTORNEY'S DOCKET NO. PHD 99-099
TRANSMITTAL LETTER TO THE UNITED STATES DESIGNED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371	U.S. Application No. (if known, see 37 CFR 1.5) 09/555305

INTERNATIONAL APPLICATION NO	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/EP99/07012	SEPTEMBER 17, 1999	SEPTEMBER 30, 1998 and August 5, 1999

TITLE OF INVENTION
ENCODING METHOD FOR CARRYING OUT CRYPTOGAPHIC OPERATIONS

APPLICANT(S) FOR DO/EO/US
STEFAN PHILIPP

Applicant(s) herewith submit to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. [X] This is a FIRST submission of items concerning a filing under 35 U.S.C. 371.

2. [ ] This is a SECOND or SUBSEQUENT submission of items concerning a filing under 35 U.S.C. 371.

3. [X] This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).

4. [ ] A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.

5. [X] A copy of the International Application as filed (35 U.S.C. 371 (c)(2))
   a. [X] is transmitted herewith (required only if not transmitted by the International Bureau).
   b. [ ] has been transmitted by the International Bureau.
   c. [ ] is not required, as the application was filed in the United States Receiving Office (RO/US).

6. [ ] A translation of the International Application into English (35 U.S.C. 371(c)(2))

7. [ ] Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. [ ] are transmitted herewith (required only if not transmitted by the International Bureau).
   b. [ ] have been transmitted by the International Bureau.
   c. [ ] have not been made; however, the time limit for making such amendments has NOT expired.
   d. [X] have not been made and will not be made.

8. [ ] A translation of the amendment to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).

9. [X] An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).

10. [ ] A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. Below concern document(s) or information included:

11. [ ] An Information Disclosure Statement under 37 C.F.R. 1.97 and 1.98.

12. [X] An assignment document for recording. A separate cover sheet is compliance with 37 C.F.R. 3.28 and 3.31 is included.

13. [X] A FIRST preliminary amendment.
    [ ] A SECOND OR SUBSEQUENT preliminary amendment.

14. [ ] A substitute specification.

15. [ ] A change of power of attorney and/or address letter.

16. [X] Other items or information:
    Charge Authorization

EL297131917US

MAY 26, 2000

FEE IS BEING
POSTAL SERVICE
EXPRESS" SERVICE
AND
DOCUMENTS AND
37 C.F.R. 1.10.

Josephine Cangelosi

(37 CFR)

Josephine Cangelosi

S:\pw\mu25pwj0.cn0

U.S. APPLICATION NO. (If known, see 37 C.F.R. 1.5) 09/555305	INTERNATIONAL APPLICATION NO. PCT /EP99/07012	ATTORNEY'S DOCKET NUMBER PHD 99-099

17 [x] The following fees are submitted:

BASIC NATIONAL FEE (37 C.F.R. 1.492(A)(1)-(5)):

		CALCULATIONS (PTO USE ONLY)
Search Report has been prepared by the EPO or JPO	$940.00	
International preliminary-examination fee paid to USPTO (37 C.F.R. 1.482)	$720.00	
No international preliminary examination fee paid to USPTO (37 C.F.R. 1.482) but international search fee paid to USPTO (37 C.F.R. 1.445(a)(2)	$760.00	
Neither international preliminary examination fee (37 C.F.R. 1.482) nor international search fee (37 C.F.R. 1.445(a)(2)) paid to USPTO	$970.00	
International preliminary examination fee paid to USPTO (37 C.F.R. 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4)	$ 96.00	
ENTER APPROPRIATE BASIC FEE AMOUNT =		$970.00

Surcharge of $130.00 for furnishing the oath or declaration later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 C.F.R. 1.492(e)).	$	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total Claims	14 - 20 =		X $ 18.00	$	
Independent claims	2 - 3 =		X $ 78.00	$	
MULTIPLE DEPENDENT CLAIMS (if applicable)			+ $260.00	$	

TOTAL OF ABOVE CALCULATIONS =	$970.00	
Reductions by 1/2 for filing by small entity, if applicable. Verified Small Entity Statement must also be filed (Note 37 C.F.R. 1.9, 1.27, 1.28)	$	
SUBTOTAL =	$970.00	
Processing fee of $130.00 for furnishing the English translation later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 C.F.R. 1.492(f)). +	$	
TOTAL NATIONAL FEE =	$	
Fee for recording the enclosed assignment (37 C.F.R. 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 C.F.R. 3.28,3.31). $40.00 per property +	$ 40.00	
TOTAL FEES ENCLOSED =	$1,010.00	
	Amount to be Refunded	$
	Charged	$

a. [ ] A check in the amount $_____ to cover the above fees is enclosed.

b. [X] Please charge my Deposit Account No. 14-1270 in the amount of $ 1,010.00 to cover the above fees. A duplicate copy of this sheet is enclosed.

c. [X] The Commissioner is hereby authorized to charge any additional fee, with the exception of the Base Issue Fee, which may be required, or credit any overpayment to Deposit Account No. 14-1270. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 C.F.R. 1.494 or 1.495 has not been met, a petition to revive (37 C.F.R. 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Corporate Patent Counsel
Philips Electronics North America Corporation
580 White Plains Road
Tarrytown, NY 10591

(SIGNATURE)

Daniel J. Piotrowski
(NAME)

42,079
(REGISTRATION NUMBER)

DATE OF MAILING:

5/26/00

S:\pw\mu25pwj0.cn0

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

STEFAN PHILIPP

Serial No.

Filed: Concurrently

Atty. Docket

PHD 99-099

ENCODING METHOD FOR CARRYING OUT CRYPTOGRAPHIC OPERATIONS

Honorable Commissioner of Patents and Trademarks
Washington, D.C. 20231

PRELIMINARY AMENDMENT

Sir:

Prior to calculation of the filing fee and examination, please amend the above-identified application as follows:

IN THE CLAIMS

Please amend claims 3-7 and 12-14 as follows:

Claim 3, line 1, delete "or 2".

Claim 4, line 1, change "one of the preceding Claims" to --Claim 1--.

Claim 5, line 1, change "one of the preceding Claims" to --Claim 1--.

Claim 6, line 1, change "one of the preceding Claims" to --Claim 1--.

Claim 7, line 1, change "one of the preceding Claims" to Claim 1--.

Claim 12, line 1, change "one of the Claims 8 to 11" to --Claim 11--.

Claim 13, line 1, change "one of the Claims 8 to 12" to

--Claim 12--.

Claim 14, line 1, change "one of the Claims 8 to 13" to

--Claim 13--.

REMARKS

The claims are amended to remove multiple dependency without change in scope.

Entry of the Amendment is respectfully requested.

Respectfully submitted,

By _____

Daniel J. Piotrowski, Reg. 42,079
Attorney
(914) 333-9624

Encoding method for carrying out cryptographic operations.

Technical field

The invention relates to an encryption method as disclosed in the introductory part of Claim 1 wherein at least one cryptographic sub-operation $y_i = f_i(x_i,k_i)$ is performed on data x_i, k_i which are digitally stored as data bit words, the relevant result or intermediate results y_i being digitally stored or buffered as data bit words. The invention also relates to an encryption device as disclosed in the introductory part of Claim 8 which includes a processor and registers R_i, the processor performing at least one cryptographic sub-operation $y_i = f_i(x_i,k_i)$ on operands x_i, k_i which are digitally stored as data bit words in the registers R_i of the encryption device, the relevant result or intermediate results y_i being digitally stored or buffered as data bit words in the registers R_i of the encryption device.

State of the art

Cryptographic operations are carried out in many data processing apparatus so as to protect the operation of such apparatus or the data transported in the apparatus. The arithmetic operations required for this purpose are carried by standard processors as well as by dedicated crypto processors. A typical example of the latter processor is formed by a chip card or an IC card. As is shown in Fig. 1, for such cryptographic calculations it is often necessary to initialize relevant storage sections or registers of the data processing apparatus with operands x_i, k_i. During the i^{th} calculation intermediate results y_i are possibly stored in storage sections or registers R_i or subsequently the result of the calculation is stored in storage sections or registers for further processing. The register R_i is situated between a preceding i^{th} cryptographic calculation and a subsequent $(i+1)^{th}$ cryptographic operation. The data x_i, k_i or intermediate results y_i used in this context customarily constitute security-relevant information such as, for example, cryptographic keys or operands.

In order to calculate the cryptographic algorithms the data processing apparatus form logic combinations of operands k_i or intermediate results y_i or x_i, x_{i+1}. Depending on the technology used, such operations, notably the loading of the storage sections or registers with data, lead to an increased current consumption of the data processing apparatus. In the case of complementary logic, for example CMOS, an increase of

the current consumption occurs when the value of a bit storage cell changes, i.e. when its value changes from "0" to "1" or from "1" to "0". The increase of the consumption is then dependent on the number of bit positions changed in the memory or register. In other words, the loading of a previously erased register causes an increase of the current consumption which is proportional to the Hamming weight of the operand (= number of bits having the value "1") or to the difference in the Hamming weight. Analysis of such a current variation could thus enable extraction of information concerning the operations executed, thus enabling successful crypto analysis of secret operands such as, for example, cryptographic keys. For example, in the case of very small signal variations, adequate information could be extracted by carrying out a plurality of current measurements on the data processing apparatus. On the other hand, a plurality of measurements could also enable a possibly required differentiation. This type of crypto analysis is also called "Differential Power Analysis" whereby an outsider could successfully perform a possibly unauthorized crypto analysis of the cryptographic operations, algorithms, operands or data purely by observing changes in the current consumption of the data processing apparatus.

From US 5,297,201 it is known to combine a high frequency radiating computer with a device which also radiates high frequency similar to that of the computer. As a result, unauthorized third parties can no longer decode the high-frequency radiated by the computer. This system, however, cannot prevent crypto analysis by a third party having direct access to the computer.

In order to eliminate a correlation in chip cards between the output of a result of a cryptographic operation or a transfer of key information for a cryptographic operation and the cryptographic operation itself, it is known from Patent Abstracts of Japan 10069222A to delay the result of the cryptographic operation or the transfer of the key information for the cryptographic operations. However, this system can also be analyzed by way of Differential Power Analysis, because the delayed data transfer also becomes apparent in the current consumption of the data processing apparatus.

Implementation of the invention, object, solution, advantages

It is an object of the present invention to provide an improved method and an improved device of the kind set forth which eliminate the described drawbacks and effectively prevent crypto analysis by observation of current consumption of a data processing apparatus.

This object is achieved by a method of the kind set forth which is characterized as disclosed in Claim 1.

To this end, according to the invention at option at least one of the data x_i, k_i and/or the result or at least one intermediate result y_i is bit-wise complemented to $\bar{y} = f(\bar{x}_i, \bar{k}_i)$ and/or $\bar{y}_i$ or not, depending on a control signal r_i which is based on random numbers.

This offers the advantage that other bit series are processed or stored in the case of repeated execution of the same cryptographic operation, so that the respective execution of a cryptographic operation or several cryptographic operations produce different current variations in the data processing apparatus. Irrespective of the actual value of the sub-results, in the case of repeated execution of the overall calculation it is thus achieved that each data path changes the same number of times from "0" to "0", from "0" "1", from "1" to "0" and from "1" to "1" in the case of a pure random number series or practically the same number of times in the case of a pseudo-random number series. However, because the control signal r_i based on random numbers is not known or predetermined, there will be no correlation between the current variations and the bit values of the data and results, so that Differential Power Analysis no longer leads to successful crypto analysis. In other words, the mean current consumption of the overall operation does not contain usable information concerning the sub-operands or intermediate results used in the sub-operations.

Advantageous further versions of the method are disclosed in the Claims 2 to 7.

Preferably, one or more XOR combinations (EXCLUSIVE- OR combinations) are formed during the cryptographic sub-operations.

The data contain, for example cryptographic keys and/or operands.

In a preferred version intermediate results y_i are buffered in a register R_i between the execution of successive cryptographic sub-operations and are used as an operand x_{i+1} for the subsequent cryptographic sub-operations.

In order to form an original, non-inverted value after each sub-operation, a bit series $x_{i+1} = y_i$ derived from the intermediate result y_i of a preceding sub-operation i is bit-wise complemented to $\bar{x}_{i+1}$ for a subsequent sub-operation i+1 if the data x_i, k_i of the preceding sub-operation i were bit-wise complemented.

In a particularly advantageous version at least one bit value, notably the even bit values, the odd bit values or all bit values, of a data bit word x_i, k_i or y_i are inverted during the bit-wise complementary operation. It is then particularly advantageous to perform an

inversion of bit values or bit addresses of a data bit word x_i, k_i or y_i by means of an XOR operation (EXCLUSIVE-OR operation) during the bit-wise complementary operation.

A device of the kind set forth according to the invention is provided with at least one inverter which can be controlled by a control signal r_i and serves for at least one of the data x_i, k_i and/or the result or at least one intermediate result y_i, with a random number generator which generates random numbers, as well as with a device for generating the control signal r_i on the basis of the random numbers, the controllable inverter either, in dependence on the control signal r_i, converting the bit series x_i, k_i or y_i into their bit-wise complement $\overline{x}_i$, $\overline{k}_i$ and $\overline{y}_i$, respectively, or leaving them unchanged.

This offers the advantage that other bit sequences are processed or stored in the case of repeated execution of the same cryptographic operation, so that other current variations occur in the data processing apparatus during the respective execution of the cryptographic operation or cryptographic operations. Irrespective of the actual value of the sub-results, in the case of repeated execution of the overall calculation it is thus achieved that each data path changes the same number of times from "0" to "0", from "0" to "1", from "1" to "0" and from "1" to "1" in the case of a pure random number series or practically the same number of times in the case of a pseudo-random number series. However, because the control signal r_i based on random numbers is not known or predetermined, there will be no correlation between the current variations and the bit values of the data and results, so that Differential Power Analysis no longer leads to successful crypto analysis. In other words, the mean current consumption of the overall operation does not contain usable information concerning the sub-operands or intermediate results used in the sub-operations.

Advantageous further embodiments of the device are described in the Claims 9 to 14.

In a preferred embodiment at least one register R_i is succeeded by an inverter which receives the same control signal r_i as the inverter for the data x_i, k_i which precedes the i^{th} sub-operation. The inverter succeeding a register R_i of the i^{th} sub-operation is preferably combined with an inverter for input data x_{i+1} which precedes the subsequent $(i+1)^{th}$ sub-operation. The combined inverter preferably receives the control signal r_i of the preceding i^{th} sub-operation as well as the control signal r_{i+1} of the subsequent $(i+1)^{th}$ sub-operation.

The data contain, for example, cryptographic keys and/or operands.

In a preferred embodiment a register R_i stores an intermediate result y_i of the preceding i^{th} sub-operation between a preceding i^{th} sub-operation and a subsequent $(i+1)^{th}$

sub-operation and forwards this intermediate result as an input value x_{i+1} to the subsequent $(i+1)^{th}$ sub-operation.

Preferably, the bit-wise complementary operation inverts at least one bit value, notably the even bit values, the odd bit values or all bit values, of a data bit word x_i, k_i or y_i.

Brief description of the drawings

The invention will be described in detail hereinafter with reference to the accompanying drawings. Therein:

Fig. 1 shows a flow chart of a part of a cryptographic operation according to the state of the art,

Fig. 2 shows a flow chart of a part of a first preferred version of a cryptographic operation according to the invention, and

Fig. 3 shows a flow chart of a part of a second preferred version of a cryptographic operation according to the invention.

Preferred implementation of the invention

In the first preferred version of an encryption method according to the invention as shown in Fig. 2 a cryptographic overall operation is performed by way of a chain of sub-operations $f_i(x_i,k_i)$ in which one or more logic XOR (EXCLUSIVE OR) combinations are formed. The Figure shows two sub-operations, i.e. the i^{th} sub-operation 10 and the $(i+1)^{th}$ sub-operation 12, each sub-operation being executed by an arithmetic unit. Each sub-operation 10, 12 is succeeded by a storage cell or a register R_i 14 and a storage cell or a register R_i 16, respectively. Each sub-operation 10, 12 has as its input value data x_i, x_{i+1} as well as an operand k_i, k_{i+1}, both being available as data bit words.

Each sub-operation 10, 12 is preceded by a respective controllable inverter 18 and 20 for the data x_i, x_{i+1}, respectively, as well as by a controllable inverter 22, 24 for the operands k_i, k_{i+1}. Furthermore, for each sub-operation 10, 12 the relevant register R_i 14 and R_{i+1} 16 is succeeded by a controllable inverter 26, 28 for the intermediate result y_i, y_{i+1}, said intermediate result being propagated by the relevant register R_i 14 and R_{i+1} 16 to a subsequent sub-operation 12 as input data x_{i+1} and x_{i+1}, respectively. The inverters 18 to 28 can be controlled by a control signal r_i and r_{i+1}, respectively, in such a manner that at option they bit-wise complement the associated data bit words or not, depending on the relevant control signal r_i and r_{i+1}, respectively. All inverters 18, 22, 26 and 20, 24, 28 of a sub-operation 10 and 12, respectively, then receive the same control signal r_i and r_{i+1},

respectively. In other words, the decision whether an inversion of the relevant input values of the inverters 18 to 28 is performed or whether the input values traverse the inverters 18 to 28 in non-processed form is taken by the additional control signal r_i and r_{i+1}, respectively. This arrangement of registers 14, 16 between sub-operations 10, 12 is used particularly when the sub-operations 10, 12 are calculated successively in time by one and the same unit so that the sub-results must be buffered.

The control signal is controlled by random values from a random generator in such a manner that, depending on the value of the random numbers, the sub-operation yields either the original result y = f(x,k) or the bit-inverted result $\overline{y} = \overline{f}(\overline{x}, \overline{k})$. It is thus achieved that the calculation as well as the storage of the data in the registers R_i 14, 16 takes place either by way of original values or bit-inverted values. In the case of repeated execution of the overall calculation it is thus achieved that each data path changes over the same number of times from "0" to "0", from "0" to "1", from "1" to "0" and from "1" to "1", irrespective of the actual value of the sub-results. The mean current consumption of the overall operation, consequently, does not contain useful information concerning the sub-operands k_i or intermediate results y_i involved in the sub-operations 10, 12. The inverter 26, 28 succeeding the registers 14, 16 restores the original, non-inverted value again for the next sub-operation 12 again.

The second preferred version of the encryption method according to the invention as shown in Fig. 3 corresponds to the first version shown in Fig. 2, the only difference being that the inverters 26, 28 succeeding the registers 14, 16 are combined with the respective input inverter 20 of the next stage 12 so as to form an inverter 30.

The inverters invert, for example, only a part of the bit values of the relevant data bit word. For example, only the even or the odd bit words or bit addresses are inverted. The bit values are inverted, for example, by means of an XOR (EXCLUSIVE OR) operation.

CLAIMS:

1. An encryption method wherein at least one cryptographic sub-operation $y_i = f_i(x_i,k_i)$ is performed on data x_i, k_i which are digitally stored as data bit words, the relevant result or intermediate results y_i being digitally stored or buffered as data bit words, characterized in that

at option at least one of the data x_i, k_i and/or the result or at least one intermediate result y_i is bit-wise complemented to $\overline{x}_i$, $\overline{k}_i$ and/or $\overline{y}_i$ or not, depending on a control signal r_i which is based on random numbers.

2. An encryption method as claimed in Claim 1, characterized in that

one or more XOR (EXCLUSIVE OR) combinations are formed during the cryptographic sub-operations.

3. An encryption method as claimed in Claim 1 or 2, characterized in that

the data contain cryptographic keys and/or operands.

4. An encryption method as claimed in one of the preceding Claims, characterized in that

intermediate results y_i are buffered in a register R_i between the execution of successive cryptographic sub-operations and are used as an operand x_{i+1} for the subsequent cryptographic sub-operations.

5. An encryption method as claimed in one of the preceding Claims, characterized in that

a bit series $x_{i+1} = y_i$ derived from the intermediate result y_i of a preceding sub-operation i is bit-wise complemented to $\overline{x}_{i+1}$ for a subsequent-operation i+1 if the data x_i, k_i of the preceding sub-operation i were bit-wise complemented.

6. An encryption method as claimed in one of the preceding Claims, characterized in that
during the bit-wise complementary operation at least one bit value, notably the even bit values, the odd bit values or all bit values, of a data bit word x_i, k_i or y_i are inverted.

7. An encryption method as claimed in one of the preceding Claims, characterized in that
bit values or bit addresses of a data bit word x_i, k_i or y_i are inverted by means of an XOR operation (EXCLUSIVE OR operation) during the bit-wise complementary operation.

8. An encryption device which includes a processor and registers R_i (14, 16), the processor performing at least one cryptographic sub-operation $y_i = f_i(x_i,k_i)$ (10, 12) on operands x_i, k_i which are digitally stored as data bit words in the registers R_i (14, 16) of the encryption device, the relevant result or intermediate result y_i being digitally stored or buffered as data bit words in the registers R_i (14, 16) of the encryption device, characterized in that
there are provided at least one inverter (18 to 28; 30) which can be controlled by a control signal r_i and serves for at least one of the data x_i, k_i and/or the result or at least one intermediate result y_i, a random number generator which generates random numbers, as well as a device for generating the control signal r_i on the basis of the random numbers, the controllable inverter (18 to 28; 30) either, in dependence on the control signal r_i, converting the bit series x_i, k_i or y_i into their bit-wise complement $\overline{x}_i$, $\overline{k}_i$ and $\hat{y}_i$, respectively, or leaving them unchanged.

9. An encryption device as claimed in Claim 8, characterized in that
at least one register (R_i(14, 16) is succeeded by an inverter (26, 28; 30) which receives the same control signal r_i as the inverter (18, 20) for the data x_i, k_i which precedes the i^{th} sub-operation (10, 12).

10. An encryption device as claimed in Claim 9, characterized in that

the inverter (26, 28) succeeding a register R_i(14, 16) of the i^{th} sub-operation (10, 12) is combined with an inverter (20) for input data x_{i+1} which precedes the subsequent $(i+1)^{th}$ sub-operation (12).

11. An encryption device as claimed in Claim 10,
characterized in that
the combined inverter (30) receives the control signal r_i of the preceding i^{th} sub-operation (10) as well as the control signal r_{i+1} of the subsequent $(i+1)^{th}$ sub-operation (12).

12. An encryption device as claimed in one of the Claims 8 to 11,
characterized in that
the data contain cryptographic keys and/or operands.

13. An encryption device as claimed in one of the Claims 8 to 12,
characterized in that
between a preceding i^{th} sub-operation (10) and a subsequent $(i+1)^{th}$ sub-operation (12) a register R_i (14, 16) stores an intermediate result y_i of the preceding i^{th} sub-operation (10) and forwards this intermediate result as an input value x_{i+1} to the subsequent $(i+1)^{th}$ sub-operation (12).

14. An encryption device as claimed in one of the Claims 8 to 13,
characterized in that
the bit-wise complementary operation inverts at least one bit value, notably the even bit values, the odd bit values or all bit values, of a data bit word x_i, k_i or y_i.

LIST OF REFERENCES

10	i^{th} sub-operation
12	$(i+1)^{th}$ sub-operation
14	register R_i
16	register R_{i+1}
18	controllable inverter for x_i
20	controllable inverter for x_{i+1}
22	controllable inverter for k_i
24	controllable inverter for k_{i+1}
26	controllable inverter for y_i
28	controllable inverter for y_{i+1}
30	combined inverter

ABSTRACT:

The invention relates to an encryption method as well as to an encryption device wherein at least one cryptographic sub-operation $y_i = f_i(x_i,k_i)$ is performed on data x_i, k_i which are digitally stored as data bit words and wherein the relevant result or relevant intermediate results y_i are digitally stored or buffered as data bit words. At option at least one of the data x_i, k_i and/or the result or at least one intermediate result y_i is bit-wise complemented to $\overline{x}_i$, $\overline{k}_i$ and/or $\overline{y}_i$ or not, depending on a control signal r_i which is based on random numbers.

Fig. 2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of , Atty. Docket

STEFAN PHILIPP PHD 99-099

Serial No. Group Art Unit:

Filed: CONCURRENTLY Examiner:

ENCODING METHOD FOR CARRYING OUT CRYPTOGRAPHIC OPERATIONS

Honorable Commissioner of Patents and Trademarks
Washington, D.C. 20231

APPOINTMENT OF ASSOCIATES

Sir:

The undersigned Attorney of Record hereby revokes all prior appointments (if any) of Associate Attorney(s) or Agent(s) in the above-captioned case and appoints:

DANIEL J. PIOTROWSKI **(Registration No. 42,079)** 3

c/o U.S. PHILIPS CORPORATION, Intellectual Property Department, 580 White Plains Road, Tarrytown, New York 10591, his Associate Attorney(s)/Agent(s) with all the usual powers to prosecute the above-identified application and any division or continuation thereof, to make alterations and amendments therein, and to transact all business in the Patent and Trademark Office connected therewith.

ALL CORRESPONDENCE CONCERNING THIS APPLICATION AND THE LETTERS PATENT WHEN GRANTED SHOULD BE ADDRESSED TO THE UNDERSIGNED ATTORNEY OF RECORD.

Respectfully,

Jack E. Haken, Reg. 26,902
Attorney of Record

Dated at Tarrytown, New York
this 24TH day of MAY, 2000
S:\PW\MU25PWI0.CN0

Fig.1

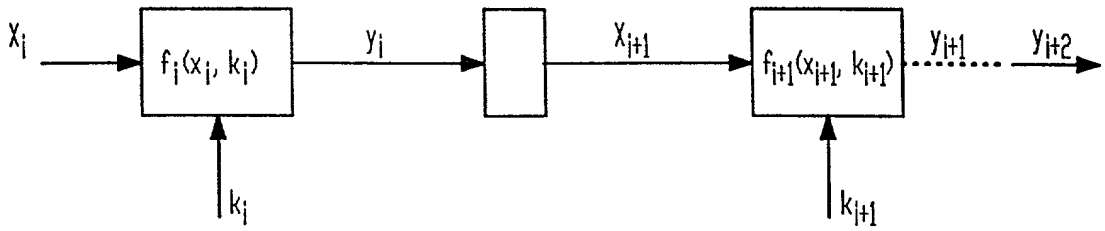


Fig.2

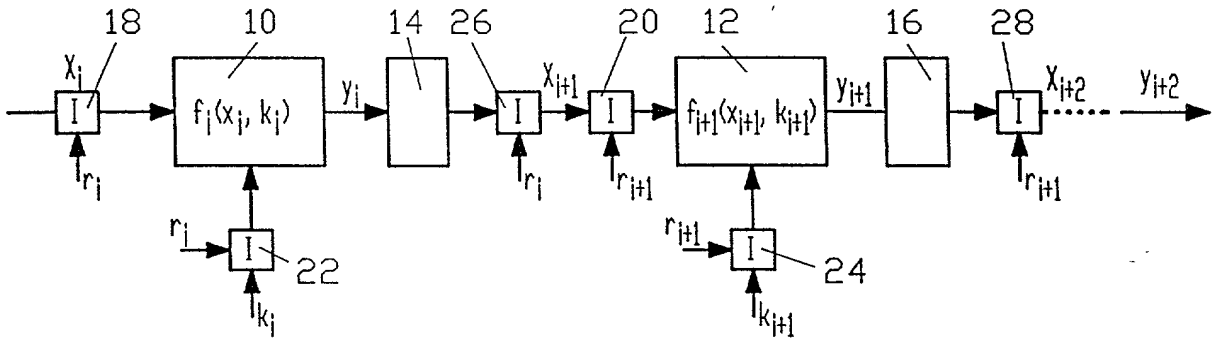
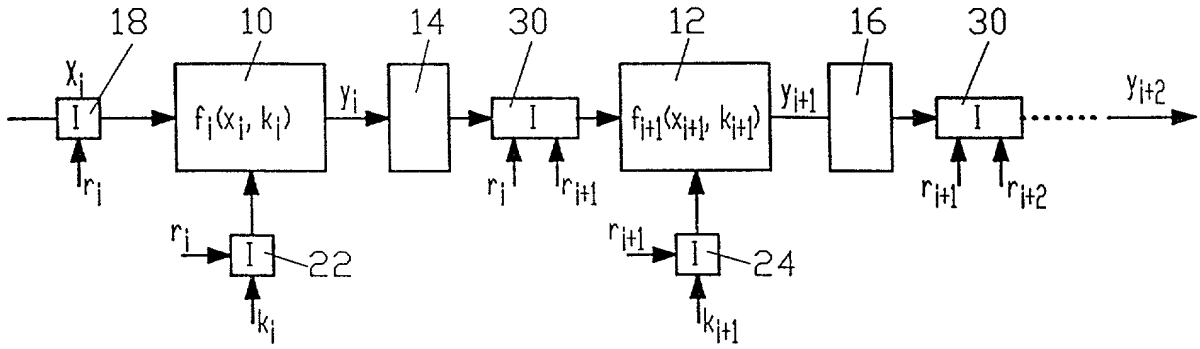


Fig.3



09/555305

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY (includes Reference to PCT International Applications)	ATTORNEY'S DOCKET NUMBER PHD 99.099 US

As a below named inventor, I hereby declare that: 526 Rec'd PCT/PTO 26 MAY 2000

My residence, post office address and citizenship are as stated next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which aa patent is sought on the invention entitled: "Encoding method for carrying out cryptographic operations" the specification of which (check only one item below):

☐ is attached hereto.

☐ was filed as United States application

Serial No _____

on _____

and was amended

on _____

☒ was filed as PCT international application

Number PCT/EP99/07012

on 17 September 1999 (17.09.99)

and was amended under PCT Article 19

on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate or of any PCT international application(s) designating at least one country other than the United States of America listed below and have identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

PRIOR FOREIGN/PCT APPLICATION(S) AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. 119:

COUNTRY	APPLICATION NUMBER	DATE OF FILING DAY, MONTH, YEAR	PRIORITY CLAIMED UNDER 35 USC 119
Germany	**19845095.8**	**30 September 1998**	**YES**
Germany	**19936918.6**	**5 August 1999**	**YES**

Combined Declaration For Patent Application and Power of Attorney (Continued) (includes Reference to PCT International Applications)	Attorneys Docket Number **PHD 99.099 US**

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) abnd/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (List name and registration number)

Algy Tamoshunas Reg. No. 27,677 Jack E. Haken, Reg. No. 26,902	Direct Telephone Calls to: (name and telephone number) (914)332-0222

201	FULL NAME OF INVENTOR	FAMILY NAME **PHILIPP**	FIRST GIVEN NAME **Stefan**	SECONDE GIVEN NAME
	RESIDENCE & CITIZENSHIP	CITY **Hamburg**	STATE OR FOREIGN COUNTRY **Germany** DEX	COUNTRY OF CITIZENSHIP **Germany**
	POST OFFICE ADDRESS	POST OFFICE ADDRESS **Eimsbütteler Chaussee 47**	CITY **20259 Hamburg**	STATE & ZIP CODE/COUNTRY **Germany**
202	FULL NAME OF INVENTOR	FAMILY NAME	FIRST GIVEN NAME	SECONDE GIVEN NAME
	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP
	POST OFFICE ADDRESS	POST OFFICE ADDRESS	CITY	STATE & ZIP CODE/COUNTRY
203	FULL NAME OF INVENTOR	FAMILY NAME	FIRST GIVEN NAME	SECONDE GIVEN NAME
	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP
	POST OFFICE ADDRESS	POST OFFICE ADDRESS	CITY	STATE & ZIP CODE/COUNTRY
204	FULL NAME OF INVENTOR	FAMILY NAME	FIRST GIVEN NAME	SECONDE GIVEN NAME
	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP
	POST OFFICE ADDRESS	POST OFFICE ADDRESS	CITY	STATE & ZIP CODE/COUNTRY
205	FULL NAME OF INVENTOR	FAMILY NAME	FIRST GIVEN NAME	SECONDE GIVEN NAME
	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP
	POST OFFICE ADDRESS	POST OFFICE ADDRESS	CITY	STATE & ZIP CODE/COUNTRY
206	FULL NAME OF INVENTOR	FAMILY NAME	FIRST GIVEN NAME	SECONDE GIVEN NAME
	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP
	POST OFFICE ADDRESS	POST OFFICE ADDRESS	CITY	STATE & ZIP CODE/COUNTRY

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true: and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 if Title 18 of the United states Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

SIGNATURE OF INVENTOR 201	SIGNATURE OF INVENTOR 202	SIGNATURE OF INVENTOR 203
Stef Ph.I.		
DATE April 20, 2000	DATE	DATE
SIGNATURE OF INVENTOR 204	SIGNATURE OF INVENTOR 205	SIGNATURE OF INVENTOR 206
DATE	DATE	DATE